UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/731,509	12/07/2000	Thomas Schaeck	DE919990082	1249

46369 7590 11/30/2010

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2493	

MAIL DATE	DELIVERY MODE
11/30/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte THOMAS SCHAECK and MICHAEL WASMUND

Appeal 2009-007326
Application 09/731,509[1]
Technology Center 2400

Before JAMES D. THOMAS, HOWARD B. BLANKENSHIP, and JEAN R. HOMERE, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL[2]

---

[1] Filed on December 7, 2000. This application claims foreign priority to application 99124724.8, filed December 11, 1999. The real party in interest is International Business Machines Corp. (App. Br. 2.)

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) (2002) from the Examiner's final rejection of claims 16 through 20 and 22 through 33. (App. Br. 7; *see also* Claims App'x.) Claims 1 through 15, 21, and 34 through 47 have been cancelled. (*Id.*) We have jurisdiction under 35 U.S.C. § 6(b) (2008).

We reverse.

Appellants' Invention

Appellants invented a method for providing card holder verification for a chip card or smart card without the card holder providing a personal identification number ("PIN"). (Spec. 1, ll. 12-18; *id.* at 3, ll. 4-14.)

Illustrative Claim

Independent claim 16 further illustrates the invention as follows:

> 16. A method of controlling card holder verification, said method comprising:
>
> checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the checking comprises comparing by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device; and
>
> if the checking indicates the presence of the trusted association, then performing card holder verification separate from the comparing using the card and without a holder of the card providing information by providing another identifier to the card from the at least one device for comparing by the card to a second identifier stored on the card that is different from the first identifier, otherwise, if the checking indicates no trusted association, then involving the holder of the card in performing card holder verification by the card.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Rikuna	4,752,678	Jun. 21, 1988
Nakamura	5,917,168	Jun. 29, 1999
Risafi	6,473,500 B1	Oct. 29, 2002 (filed Oct. 28, 1998)

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

Claims 16 through 20, 22, 25, and 28 through 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Rikuna and Nakamura.

Claims 23, 24, 26, and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Rikuna, Nakamura, and Risafi.

Appellants' Contentions

Appellants contend that Rikuna fails to disclose storing one or more identifiers in the terminal. (App. Br. 10-11.) In particular, Appellants argue that Rikuna's disclosure of storing both the Primary Account Number ("PAN") and the encrypted PAN ("EN-PAN") in the first card does not teach "one or more identifiers stored in the at least one device," as recited in independent claim 16. (*Id.* at 11.) According to Appellants Rikuna discloses storing the EN-PAN in the card and, therefore, the decrypted PAN comes from the card instead of the terminal. (*Id.* at 11-12.) Appellants also contend that independent claim 16 is directed to one card, whereas Rikuna discloses two separate cards. (Reply Br. 3.)

Further, Appellants argue that Rikuna's disclosure of entering a PIN in a second card, or remote PIN entry card, always amounts to providing a

PIN entered by the card holder and, therefore, does not teach performing card holder verification *without the holder of the card providing information*. (App. Br. 12.) According to Appellants, Rikuna discloses that user verification is done by the card holder either entering a PIN into the remote PIN entry card, or if the other card is directly connected to the terminal, the card holder entering the PIN directly into the terminal. (Reply Br. 2.) Therefore, Appellants contend that the card holder is always providing a PIN. (*Id.*) Moreover, Appellants disagree with the Examiner's position that the card holder does not provide information for card holder verification because Rikuna discloses entering the PIN in the remote PIN entry card before it is taken by the waitress. (*Id.*) Appellants allege that there is no express or implied time frame for card holder verification recited in independent claim 16. (*Id.* at 2-3.)

Additionally, Appellants contend that Nakamura discloses that if the terminal and card do not authenticate, the card holder cannot utilize the card. (App. Br. 12.) Consequently, Appellants argue that Nakamura does not teach involving the holder of the card in performing card holder verification if the checking indicates no trusted association. (*Id.*) Moreover, Appellants allege that Rikuna's disclosure of eliminating the need for a card holder to enter a PIN into a terminal, but not eliminate the PIN altogether, is at odds with Nakamura's disclosure of not always requiring PIN entry. (Reply Br. 4.) Appellants also contend that Nakamura's disclosure of not requiring a PIN for a transaction amount lower than a set value is not the same as requiring a trusted association. (*Id.*) That is, Appellants argue that Nakamura's disclosure amounts to a decision not to check for a trusted

association below the set value, but instead assuming the risk of fraud at that level. (*Id.*)

Examiner's Findings and Conclusions

The Examiner finds that Rikuna discloses a decryptor within the terminal that decrypts the EN-PAN to generate a decrypted PAN, which is stored in the latch of the terminal, and, subsequently, compares the decrypted PAN with the PAN stored in the PAN memory of a user's card. (Ans. 17-18.) Therefore, the Examiner finds that Rikuna's disclosure teaches both "a first identifier stored on the card" and "one or more identifiers stored in the at least one device," as recited in independent claim 16. *(Id.* at 18.)

Further, the Examiner finds that time of verification and the verification process of independent claim 16 can be construed as the same. (Ans. 19.) The Examiner finds that the objective of Rikuna is to not allow a user to directly input a PIN during card holder verification. (*Id.*) Consequently, the Examiner finds that Rikuna discloses allowing a user to record a PIN to be stored in a remote PIN entry card a long time before the verification process takes place. (*Id.*) The Examiner also finds that Rikuna discloses that the verification process occurs after a waitress picks up both cards and inserts both cards into a terminal. (*Id.* at 20.) Therefore, the Examiner finds that Rikuna discloses performing the comparison step at the terminal utilizing both cards without the card holder inputting information into the terminal. (*Id.* at 20-21.)

Additionally, the Examiner finds that Nakamura's disclosure of requiring PIN entry only when the amount of a transaction exceeds a preselected floor limit teaches "if the checking indicates no trusted

association, then involving the holder of the card in performing card holder verification by the card," as recited in independent claim 16. (*Id.* at 21.)

II. ISSUE

Have Appellants shown that the Examiner erred in concluding that the combination of Rikuna and Nakamura renders independent claim 16 unpatentable? In particular, the issue turns on whether the proffered combination teaches the following claim limitations:

(a) "performing card holder verification…without a holder of the card providing information…," as recited in independent claim 16; and

(b) "if the checking indicates no trusted association, then involving the holder of the card in performing card holder verification by the card," as recited in independent claim 16.

III. FINDINGS OF FACT

The following Findings of Fact ("FF") are shown by a preponderance of the evidence.

Rikuna

1. Rikuna generally relates to an integrated circuit ("IC") card system that utilizes an IC card and a card terminal to pay charges, such that the location to pay charges is remote from the position where a card holder exists. (Col. 1, ll. 8-13.)

2. Rikuna's figure 8 depicts that during or after completion of eating at a restaurant, a card holder utilizes a bill to calculate an amount of payment and inputs both a calculated total amount of payment ("AMT") and personal identification number (PIN) into a remote PIN entry card (21).

(Col. 6, ll. 2-11.) Thereafter, Rikuna discloses that the card holder inserts his/her user's card (11) and remote PIN entry card (21), which stores both the PIN and AMT data, into the first and second card keepers (83A & 83B) of a card binder (81). (*Id.* at ll. 11-15.) Rikuna discloses that a waitress in the restaurant retrieves the card binder (81), brings the card binder to a cash register, and inserts the remote PIN entry card (21) into the card inlet (15) of card terminal (12). (*Id.* at ll. 16-19.) Rikuna discloses transferring the PIN data which was inputted by the card holder into the remote PIN entry card (21) to card terminal (12), thereby eliminating the need for the card holder to visit the cash register and key input the PIN. (Col. 8, ll. 58-66.)

Nakamura

3. Nakamura generally relates to performing on-line revaluation of token information stored in IC cards and, in particular, to performing such revaluation in a private location. (Col. 1, ll. 9-14.)

4. Nakamura discloses eliminating PIN validation in order to speed up the processing of a transaction. (Col. 5, ll. 64-66.) In particular, Nakamura discloses only requiring PIN entry when the amount of a transaction exceeds a preselected floor limit. (Col. 6, ll. 8-10.)

IV. ANALYSIS

Claim 16

Independent claim 16 recites, in relevant parts:

> 1) performing card holder verification…without a holder of the card providing information…; and 2) if the checking indicates no trusted association, then involving the holder of the card in performing card holder verification by the card.

As detailed in the Findings of Fact section above, Rikuna discloses utilizing an IC card and a terminal to pay charges, such that the terminal is remote from the position of the card holder. (FF 1.) In particular, Rikuna discloses that upon finishing eating at a restaurant, a card holder inputs both the AMT and PIN into a remote PIN entry card. (FF 2.) After a waitress retrieves both the card holder's IC card and the remote PIN entry card, the waitress inserts the remote PIN entry card into a register or terminal to thereby transmit the PIN and AMT data to the terminal. (*Id.*) Accordingly, Rikuna discloses that the card holder does not need to visit the terminal and key input the PIN. (*Id.*)

At best, we find that Rikuna's disclosure teaches verifying a card holder's IC card by taking both the IC card and a remote PIN entry card to a terminal, such that the card holder does not need to visit the terminal and key input a PIN. Although Rikuna discloses that the card holder does not need to visit the terminal and key input a PIN, the card holder verification process still requires that the card holder always enters his/her PIN into the remote PIN entry card. Thus, we find that Rikuna fails to teach or suggest "performing card holder verification…without a holder of the card providing information…," as recited in independent claim 16.

Moreover, Nakamura discloses performing revaluation of token information stored in an IC card at a private location. (FF 3.) In particular, Nakamura discloses speeding up the processing of a transaction by eliminating PIN validation. (FF 4.) Further, Nakamura discloses only requiring PIN entry when the amount of a transaction exceeds a preselected floor limit. (*Id.*)

We find that Nakamura's disclosure teaches, at best, requiring a card holder of an IC card to enter a PIN into a terminal only when the amount of a transaction exceeds a threshold value. However, we note that a threshold value is not a trusted associated. We agree with Appellants that Nakamura's disclosure of not requiring a PIN for a transaction amount lower that a threshold value amounts to not checking for a trusted association, but instead assuming the risk of fraud at that level. (Reply Br. 4.) Further, we find that Rikuna fails to cure the noted deficiencies in Nakamura. Thus, we find that the proffered combination also fails to teach or suggest "if the checking indicates no trusted association, then involving the holder of the card in performing card holder verification by the card," as recited in independent claim 16.

Since Appellants have shown at least one error in the Examiner's rejection of independent claim 16, we need not address Appellants' other arguments. It follows that Appellants have shown that the Examiner erred in concluding that the combination of Rikuna and Nakamura renders independent claim 16 unpatentable.

Claims 17 through 20 and 22 through 33

Since independent claim 33, and dependent claims 18 through 20 and 22 through 32, also incorporate the limitations discussed above, we find that Appellants have also shown error in the Examiner's rejection of these claims for the reasons set forth in our discussion of independent claim 16.

V. CONCLUSION OF LAW

Appellants have shown that the Examiner erred in rejecting claims 16 through 20 and 22 through 33 as being unpatentable under 35 U.S.C. § 103(a).

VI. DECISION

We reverse the Examiner's decision to reject claims 16 through 20 and 22 through 33.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

REVERSED

Vsh

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203